Mixed Critical Systems

Background

Testing, validation, verification, and certification of unmanned avionic systems, with components of different criticality are critical barriers to rapid insertion, growth and effective utilization of unmanned assets within the military and civilian communities. Increasing software complexity multiplies the cost of its testing and validation to a degree that becomes prohibitive. The adoption and advancement of new and emerging technologies has been hindered by lack of significant evolution of standard certification processes. This is especially true for mixed criticality architectures, which are increasingly common on unmanned aircraft capable of flying and managing missions autonomously. Characterization and the development of acceptable and cost effective methods of software, component, system, and network certification remain a stumbling block to reach the desired NIT goals in the area of High Confidence Software and Systems (HCSS).

Mixed Criticality

Mixed criticality is the concept of allowing applications at different levels of criticality to interact and co-exist on the same computational platform. Unfortunately, certification of such systems is more difficult, because it requires that even the components of less criticality be certified at the highest criticality level. One approach to achieve mixed criticality without increased certification expense and effort is to use ARNC653 time and space partitioning. The ARNC653 approach allocates a predefined faction of CPU time and memory of the whole system to each partition. By defining and restricting available time and space resources by partition; this prevents faults and failures in one partition from corrupting another partition leading to system failures. Each partition can be certified to a different known level of criticality.

An equivalent construct in the security arena is that of Multiple Independent Levels of Security (MILS). MILS is a departure from present operating system architectures that were designed prior to the Internet, when there was little threat of network attacks. As a result, these early systems did not incorporate security as a design requirement and use “fail first, patch later approach to inevitable failures and intrusions. MILS allows the co-execution of various application images, at differing levels of security, with dedicated hardware with strongly controlled data flow between them. A “separation kernel” provides the MILS policy enforcement layer.

Both approaches demand significant investments in time and effort to effectively meet the appropriate certification levels and thus constitute a significant barrier to the adoption of unmanned systems.

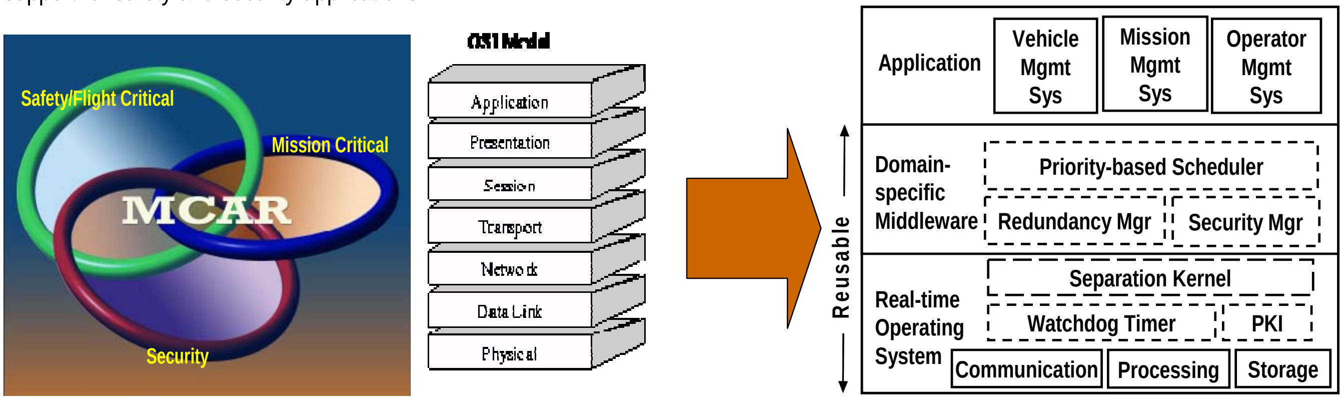
Mixed Criticality Challenges

- Certification of Compostable components: Future systems are likely to be constructed from compostable components with known levels of certifiability. The challenge is to identify, develop and implement both a certification process and a compostability framework that will support compostable and incremental certification.
- Certification by Design: A means of identifying and assessing the “certifiability” of a component, even before it is implemented, is a necessary condition, in order to support both compostable and incremental certification. This includes both formal and analytical methods that seek to define a design process that embeds attributes of certifiability with it.
- Reconfigurable Systems: It is inherently difficult to bind the decision space of an avionics system that has the ability to reconfigure itself under certain failures or contingencies. This poses a challenge to certifying reconfigurable systems form a cost, effort and complexity standpoint.
- Fault Tolerant Systems: Modern mixed critical systems need to exhibit a high degree of fault-tolerance. Canonical or generic approaches to implementing fault tolerance in avionics systems are extremely hard to come by. Consequently, it is even harder to define an approach to certifying the behavior of such systems. Nevertheless, a more flexible process than the one currently available is needed urgently.

Ongoing Efforts

The MCAR program is example of a multi-agency and multi-disciplinary program combining the expertise of government, industry, and academia to address a common issue of mixed criticality certification. The Air Force Research Laboratory (AFRL) joined with the National Science Foundation (NSF) created the MCAR, or Mixed Criticality Architecture Requirements project, which aims to build industry consensus on the problems, challenges and potential solutions to the certification of mixed critical systems. With a strong active commitment of all stakeholders, whether industry, government, or academic; the MCAR project combines the experience and expertise of three major industry players (Boeing, Lockheed, and Northrop Grumman), industry representative experts in real-time operating systems and middleware frameworks, as well as academic experts addressing future mixed criticality architectures with a focus on certification and security.

MCAR aims at trying to solve the problems of certification of today's software by unifying embedded system development with enhanced middleware components development to expand the system certification process. MCAR places an emphasis on component and subsystem reuse by migrating common requirements from the individual applications into a common component-based middleware layer. Combined with upgradeable hardware building blocks, the development of a reusable middleware level provides a path to cost effective certification. The MCAR Program layered software approach consists of a high confidence Real-Time Operating System (HC-RTOS) and Domain-specific Management System specific Middleware. The HCRTOS provides the foundation for the architecture, providing the low-level fault tolerance and separation support for safety and security applications.



Desired NIT Capabilities

In order to address the challenges discussed above, we believe NITRD represents a force for change that can help focus attention, direct funding and establish priorities for future infrastructure. Some of the areas of relevance are:

1. Infrastructure to support Enhanced Certification Process for the certification of emerging mixed-critical avionics systems
2. Cross-Spectrum Technology Push program to mature and transition research and technology in the area middleware frameworks for Mixed Critical systems
3. Technology push programs to develop tools and frameworks to support Cross-Vendor Assessment and evaluations of Real Time Operating Systems

NITRD Program Roles and Functions

Given the broad spectrum of players comprising NITRD, there is little doubt that with the right set of problems and focusing of effort across academia, government and industry will yield positive results. Therefore, the choices of program elements and goals, players as well as mechanisms to implement the goals are critical to its success. Some of these elements are noted below:

1. Development and execution of multi-agency and multi-disciplinary programs to mature the research in the challenge areas of Mixed Criticality
2. A concerted effort to accelerate the transition of research and technology in Cyber Physical Systems into Mixed Critical implementations, tools and frameworks into application realistic environments through a cross-agency effort. Cert.Auth + AFRL + NSF + Industry + Academia = Mixed Criticality Success
3. Targeted Steering of strategic goals, key challenges, opportunities, and research priorities; could include steering available research funding for Academia and small businesses to address Mixed Criticality challenges, as well as providing clearinghouse / dissemination mechanisms across academia, government and industry.
4. Providing a strategic goal to the Mixed Critical Systems community of building an open source test bed and framework for the assessment and evaluation of emerging best-of-breed solutions within realistic application bindings

The opinions and positions in the white papers and comments posted on this web site are those of the submitters only and do not necessarily represent those of the Federal government, the NITRD program and its participating agencies, or the National Coordination Office.